UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,206	07/31/2003	Raymond E. Ozzie	M1103.70263US00	3320

45840 7590 12/28/2007

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Best Available Copy

Office Action Summary	Application No.	Applicant(s)	
	10/161,082	ASOKAN ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-11,14-31,34-37 and 40-45* is/are rejected.

7)☒ Claim(s) *12-13,32-33,and 38-39* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to request for continued examination and remarks filed on October 26, 2007. Original application contained Claims 1-50. Applicant previously elected to withdraw Claims 46-50. Applicant previously amended Claims 1, 27, and 37. Applicant currently amended Claims 1, 3-5, 12, 14, 27, 32, and 37. Applicant cancelled Claim 2. The amendments filed on October 26, 2007 have been entered and made of record Therefore, presently Claims 1, and 3-45 are pending for consideration..

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 26, 2007 has been entered.

Allowable Subject Matter

Claims 12-13, 32-33, and 38-39 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim, objected claims, and any intervening claims.

Response to Arguments

Applicant's arguments filed on October 26, 2007 regarding previous art rejection have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, and 3-45 applicants argued that the system of cited prior art (CPA) [Koved et al. (U.S. Publication No. 2002/0161996 A1)] does not teach, the subject matter as claimed. .

This is not found persuasive. The JRE is a software bundle which consists of the Java Virtual Machine and the application and programming interface (API). The interface (API) provides a set of standard class libraries. The virtual machine and API are consistent with each other and bundled together as the JRE. This can be considered a virtual computer in which the virtual machine is the processor and the API is the user interface. Therefore, applicant argument that the DRM functions in Koved are encapsulated within the JRE, thus authentication is focused on the JRE itself, and not on the operating system nor on the rendering applications, is not persuasive because JRE itself works as a operating system for interacting with other resources (e.g. IPC) and other application in JRE environment because JRE is considered a virtual computer in which the virtual machine is the processor and the API is the user interface, therefore, there will always be an IPC connection when JRE interacts with native operative system. As a result, cited prior art does implement and teach a system and method that relates to dynamically enforcing digital rights management rules [0051-0058, and 0117-0130].

Applicants *still* have failed to identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner asserts that cited prior art(s) does teach or suggest the subject matter recited in independent and dependent claims. Accordingly, rejections for claims 1, 3-11, 14-31, 34-37 and 40-45 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-11, 14-31, 34-37 and 40-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Koved et al. (U.S. Publication No. 2002/0161996 A1).

1. Regarding Claim 1 Koved teach a method for enforcing digital rights management (DRM) rules at a terminal, comprising: receiving content and at least one voucher identifying the DRM rules at the terminal; providing on-demand authentication of an operating terminal application which is seeking access to the content, via secure communications between a DRM engine and an operating system augmented with a security manager adapted to conduct the secure communications, wherein the terminal application comprises a rendering program running

on the operating system concurrently with and independently of the DRM engine, and wherein the terminal application is already running prior to being authenticated; if the terminal application is authenticated, applying the DRM rules to determine whether the terminal application may access the content; and accessing the content by the terminal application if access is allowed in response to applying the DRM rules [0051-0058, 0117-0122, and 0129-0130].

2. Regarding Claim 27 Koved teach a method for enforcing digital rights management (DRM) rules at a terminal, comprising: requesting access to content securely stored in the terminal; requesting, by a DRAT engine, at least a portion of program text of a process identified by an inter-process communication (IPC) connection between the DRM engine and a rendering application, wherein the process corresponds to the rendering application, and wherein the rendering application comprises a program running on the operating system concurrently with and independently of the DRM engine; receiving the request for the program text by a security manager and identifying the process corresponding to the IPC connection; providing the program text to the DRM engine from the security manager; authenticating the rendering application based on the program text of the process and a certificate of the rendering application, wherein the rendering application is already operating prior to the authentication of the application; making an access control decision by the DRM engine if the rendering application is authorized to access the program text of the process; and making the content accessible to the rendering application if the access control decision is positive [0051-0058, 0117-0122, and 0129-0130].

3. Regarding Claim 37 Koved teach a terminal capable of receiving content and at least one corresponding voucher including usage rights for the content, comprising: a rendering application to provide a content request and to present the content upon access authorization; a digital rights management (DRM) engine coupled to receive the content request and to invoke a request to authenticate the rendering application in response thereto, wherein the request to authenticate the rendering application includes at least an identifier of an inter-process communication (IPC) connection opened in response to the content request; an operating system augmented with a security manager configured to receive the request to authenticate the rendering application and the IPC connection identifier, and in response to provide data uniquely associated with a process identified by the IPC connection, wherein the process correspond to the rendering application; and wherein the DRM engine further receives the data and verifies a certificate of the rendering application using the data, and if the rendering application is successfully verified, allowing the rendering application access to the content as dictated by the usage rights wherein the rendering application comprises a program running on the operating system concurrently with and independently of the DRM engine, and wherein the rendering application is already running prior to being authenticated by the security manager [0051-0058, 0117-0122, and 0129-0130].

4. Claims 2-26, 28-36, and 38-45 are rejected applied as above rejecting Claims 1, 27, and 37. Furthermore, Koved teach and describes:

A per Claim 3, wherein providing on-demand authentication of the operating terminal application comprises: invoking an authentication request at the DRM engine to retrieve at least

a portion of program text of a process identified by an inter-process communication (IPC) connection opened by the terminal application in response to a content request by the terminal application, wherein the process corresponds to the terminal application; receiving the authentication request by the security manager and identifying the process corresponding to the IPC connection; providing the program text to the DRM engine from the security manager; and verifying, by the DRM engine, the legitimacy of the terminal application by verifying a certificate of the terminal application based on the program text [0051, and 0129-0130].

A per Claim 4, wherein providing on-demand authentication of the operating terminal application comprises: invoking a certificate verification request at the DRM engine, wherein the certificate verification request is accompanied by arguments including a certificate of the terminal application and an identifier of a process corresponding to an inter-process communication (IPC) connection opened by the terminal application in response to a content request by the terminal application, wherein the process corresponds to the terminal application; receiving the certificate verification request by the security manager and verifying the certificate against a predetermined certificate value; and providing a verification indication to the DRM engine from the security manager indicating whether the certificate is correct and valid [0051, and 0129-0130].

A per Claim 5, wherein providing on-demand authentication of the operating terminal application comprises: invoking an authentication request at the DRM engine to retrieve a hash of at least a portion of program text of a process identified by an inter-process communication (IPC) connection opened by the terminal application in response to a content request by the terminal application, wherein the process corresponds to the terminal application; receiving the

authentication request by the security manager and identifying the process corresponding to the IPC connection; computing, at the security manager, the hash of the program text for each new process created; providing, from the security manager to the DRM engine, the hash of the program text corresponding to the IPC connection identified in the authentication request; and verifying, by the DRM engine, the legitimacy of the terminal application by comparing the hash of the program text with values expected by the DRM engine based on the certificate issued to the terminal application [0051, and 0129-0130].

A per Claim 6, wherein receiving content comprises receiving encrypted content, and wherein accessing the content by the terminal application comprises accessing plaintext content resulting from decrypting the encrypted content at the DRM engine [0055-0056].

A per Claim 7, further comprising requesting a content key from the security manager by the DRM engine, and wherein decrypting the encrypted content at the DRM engine comprises decrypting the encrypted content using the content key received from the security manager [0055-0056].

A per Claim 8, wherein receiving content comprises receiving encrypted content, and wherein accessing the content by the terminal application comprises: maintaining a content key at the security manager; decrypting requested blocks of the content at the security manager using the content key; and providing the requested blocks of decrypted content to the DRM engine [0105-0109].

A per Claim 9, wherein receiving content comprises receiving encrypted content, and wherein accessing the content by the terminal application comprises: requesting a content key from the security manager by the DRM engine; decrypting requested blocks of the content at the

DRM engine using the content key; and providing only requested blocks of the content to the terminal application [0055-0056].

A per Claim 10, wherein receiving content comprises receiving encrypted content, and wherein accessing the content by the terminal application comprises: providing a content key from the security manager to the terminal application; and decrypting the encrypted content by the terminal application using the content key [0051-0058].

A per Claim 11, wherein receiving content comprises receiving encrypted content, and wherein accessing the content by the terminal application comprises: providing a content key from the DRM engine to the terminal application; and decrypting the encrypted content by the terminal application using the content key [0051-0058].

A per Claim 14, wherein, further comprising: issuing a request to the security manager by the DRM engine to provide a connection to a process whose program text matches a terminal application certificate provided by the DRM engine, wherein the process corresponds to the terminal application; and returning a handle to the connection to the DRM engine [0057-0058].

A per Claim 15, wherein providing on-demand authentication of the operating terminal application comprises: invoking an authentication request at the DRM engine to retrieve at least a portion of program text of the process identified by the handle; receiving the authentication request by the security manager and identifying the process corresponding to the connection; providing the program text to the DRM engine from the security manager; and verifying, by the DRM engine, the legitimacy of the terminal application by verifying a certificate of the terminal application based on the program text [0051, and 0129-0130].

A per Claim 16, further comprising: issuing a request to the security manager by the DRM engine to provide a connection to a process whose program text matches a particular type selected from a standard set of type specified in certificates; and returning a handle to the connection to the DRM engine [0057-0058].

A per Claim 17, wherein providing on-demand authentication of the operating terminal application comprises: invoking an authentication request at the DRM engine to retrieve at least a portion of program text of the process identified by the handle; receiving the authentication request by the security manager and identifying the process corresponding to the connection; providing the program text to the DRM engine from the security manager; and verifying, by the DRM engine, the legitimacy of the terminal application by verifying a certificate of the terminal application based on the program text [0051, and 0129-0130].

A per Claim 18, further comprising verifying the DRM engine by the security manager by computing a hash of the DRM engine's code and associating the hash with private files created by the DRM engine [0051-0058].

A per Claim 19, further comprising verifying the DRM engine by the security manager by verifying the DRM engine's certificate and associating the certificate with private files created by the DRM engine [0051-0058].

A per Claim 20, further comprising: wirelessly providing the content and a voucher identifying the DRM rights to the terminal; and securely storing the content and the voucher locally at the terminal [0051-0058].

A per Claim 21, wherein the terminal is a wireless terminal, and further comprising sending the content and the at least one voucher to the wireless terminal from a second wireless terminal [Fig.2, 0051-0058].

A per Claim 22, wherein applying the DRM rules comprises analyzing usage rights provided via the voucher [0105-0109].

A per Claim 23, wherein the terminal application is a multi-part terminal application, and wherein providing on-demand authentication of the terminal application comprises providing on-demand authentication of each part of the multi-part terminal application [0051, 0117-0122, and 0129-0130.

A per Claim 24, wherein the terminal application is a multi-part terminal application, and wherein providing on-demand authentication of the multi-part terminal application comprises: invoking an authentication request at the DRM engine to retrieve program text of each part of the multi-part terminal application identified by an inter-process communication (IPC) connection opened in response; to a content request by the multi-part terminal application; receiving the authentication request by the security manager and identifying the process corresponding to the IPC connection; returning the program text of each part of the multi-part terminal application to the DRM engine from the security manager; and verifying, by the DRM engine, the legitimacy of the multi-part terminal application by verifying certificates of the terminal application based on each of the returned program texts [0051, and 0129-0130].

A per Claim 25, wherein the terminal application is a multi-part terminal application, and wherein providing on-demand authentication of the multi-part terminal application comprises: invoking an authentication request at the DRM engine to retrieve hashes of program text of each

part of the multi-part terminal application identified by an inter-process communication (IPC) connection opened in response to a content request by the multi-part terminal application; receiving the authentication request by the security manager and identifying the process corresponding to the IPC connection; computing, at the security manager, a hash for each of the program texts for each new process created; returning the hash of each part of the multi-part terminal application to the DRM engine from the security manager; and verifying, by the DRM engine, the legitimacy of the multi-part terminal application by verifying certificates of the terminal application based on each of the returned hashes [0051-0058, and 0129-0130].

A per Claim 26, wherein the terminal application is a multi-part terminal application, and wherein providing on-demand authentication of the multi-part terminal application comprises: invoking a certificate verification request at the DRM engine, wherein the certificate verification request is accompanied by arguments including a certificate for each part of the multi-part terminal application and an identifier of a process corresponding to an inter-process communication (IPC) connection opened in response to a content request by the terminal application; receiving the certificate verification request by the security manager and verifying the certificates against predetermined certificate values; and providing a verification indication to the DRM engine from the security manager indicating whether the certificates are correct and valid [0051-0058, and 0129-0130].

A per Claim 28, wherein the requested content stored in the terminal is encrypted, and further comprising: requesting, by the DRM engine, a content key for decrypting the requested content if the access control decision is positive; providing the content key to the DRM engine from the security manager; and decrypting the content at the DRM engine [0051-0058].

A per Claim 29, wherein authorizing the content comprises authorizing the decrypted content to be accessed via the IPC connection by the rendering application [Fig.2, 0051-0058, and 0129-0130].

A per Claim 30, wherein requesting access to the content comprises requesting access to the content by the rendering application [0117-0122].

A per Claim 31, wherein requesting content by the rendering application comprises invoking a content request accompanied by at least a content identifier that identifies the requested content, and the certificate: of the rendering application [0117-0122].

A per Claim 34, wherein making the content accessible to the rendering application comprises authorizing the content to be accessed by the rendering application via the IPC connection [0117-0122, and 0051-0058].

A per Claim 35, wherein, further comprising augmenting an operating system operating within the terminal to include the security manager [0105-0109].

A per Claim 36, wherein requesting the program text comprises invoking a primitive to obtain the program text, wherein the primitive is accompanied by arguments including an IPC identifier to allow the security manager to identify the process corresponding to the IPC connection [Fig.2, 0117-0122, and 0051-0058].

A per Claim 38, wherein the data uniquely associated with the process identified by the IPC connection comprises program text of the process [Fig.2, 0117-0122, and 0051-0058].

A per Claim 39, wherein the data uniquely associated with the process identified by the IPC connection comprises a hash of the program text of the process [Fig.2, 0117-0122, and 0051-0058].

A per Claim 40, wherein the content received at the terminal is encrypted, and wherein the security manager is further configured to provide a content key to the DRM engine in response to a key request by the DRM engine [Fig.2, 0105-0109, and 0051-0058].

A per Claim 41, wherein the DRM engine is further configured to decrypt the content using the content key, and to allow the rendering application access to the decrypted content as dictated by the usage rights [Fig.2, 0105-0109, and 0051-0058].

A per Claim 42, wherein the security manager is integrally implemented into the operating system kernel [Fig.2, 0105-0109, 0117-0122 and 0051-0058].

A per Claim 43, wherein the security manager is implemented outside the operating system kernel as a secure library [Fig.2, 0105-0109, 0117-0122 and 0051-0058].

A per Claim 44, wherein the terminal comprises a mobile device comprising at least one of a wireless telephone, wireless PDA, or wireless computing device [Fig.2, 0105-0109, 0117-0122 and 0051-0058].

A per Claim 45, wherein the terminal comprises a landline client terminal coupled in a server environment [Fig.2, 0105-0109, 0117-0122 and 0051-0058].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
December 21, 2007

SYED A. ZIA 12/21/2007
PRIMARY EXAMINER